Nottinghamshire County Council

Regulation of Investigatory Powers Act and Surveillance Guidance – covert surveillance, 'directed' surveillance and Covert Human Intelligence Sources (CHIS)

Contents

1. Introduction

1.1. The purpose of this guidance is to help officers understand the different types of covert surveillance that may be undertaken, and in which circumstances. It sets out the procedure to follow, and provides guidance regarding the information to be included in the relevant forms. It also explains where to go for further advice and guidance. This guidance applies across the County Council and supports the Council's Regulation of Investigatory Powers Act Policy.

2. When does this Guidance Apply? (including example scenarios)

2.1. The two principal activities that make Part II of the Regulation of Investigatory Powers Act (RIPA) applicable to the County Council are the use of "Directed (Covert) Surveillance" and the use of "Covert Human Intelligence Sources" (CHIS). The purpose of surveillance must be to prevent or detect crime.

2.2. The Council can only authorise Directed Surveillance to prevent and detect conduct which constitutes one or more criminal offences. The criminal offences must be punishable by a maximum term of at least 6 months imprisonment or be an offence relating to the sale of alcohol or tobacco to people under the age of 18.

2.3. The Council would be responsible for safeguarding the wellbeing of anyone authorised as a CHIS. The requirements are onerous, therefore legal advice must be sought straight away if CHIS circumstances have arisen or if a CHIS is contemplated. It is important that officers understand when a CHIS situation might arise and how to deal with that situation.

2.4. The provisions of RIPA apply when the Council is carrying out covert surveillance in the discharge of one of its core functions, for example trading standards investigations. There may be some circumstances where the Council considers the use of covert surveillance when RIPA does not apply, for example in its capacity as an employer, for child protection investigations, or for audit purposes. In these circumstances it is still a requirement to use the internal RIPA procedures (but not seek magistrate court approval) and further advice should be sought from the Coordinating Officer in Legal Services. Application forms should be re-labelled 'Human Rights Act' instead of 'RIPA' in these circumstances.

2.5. The following examples illustrate circumstances when RIPA may and may not apply. Further advice is available from Legal Services; circumstances always vary and each situation needs to be considered on its own merits.

2.5.1. The normal use of CCTV is not usually covert (secret) because members of the public are informed by signs that such equipment is in operation. However authorisation should be sought where it is intended to use CCTV to target a specific individual or group of individuals.

2.5.2. RIPA applies to covert surveillance of a person carrying out their professional or business affairs as well as of a person in their private family life.

2.5.3. Covertly taking a photograph to update records should be authorised.

2.5.4. When a person carries out a test purchase at a shop, this is potentially directed covert surveillance or CHIS, but it depends on the particular arrangements.

2.5.5. An immediate response to events or circumstances where it would not be reasonably practicable for a RIPA authorisation to be sought will not require authorisation. This does not include situations where the need for authorisation is neglected until it is too late to apply for it.

2.5.6. A 'drive by' may or may not need an authorisation; it depends on the particular circumstances. It is not acceptable to prescribe a minimum number of passes before an authorisation is required.

2.5.7. General observation that forms part of everyday duties, even if it involves use of equipment to reinforce normal sensory perception (eg binoculars or a camera) is not likely to be caught by RIPA, provided it's not systematic covert surveillance of an individual.

2.5.8. Placing tracking devices on County Council vehicles is not covert surveillance providing employees are properly notified.

2.5.9. Covert surveillance of a social networking site may require an authorisation for directed surveillance, or CHIS if a relationship is to be established. For more information see the section on online covert activity below.

2.5.10. Any covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or using a surveillance device, amounts to 'intrusive surveillance'. The Council may <u>not</u> authorise or undertake such surveillance.

2.5.11. Where a member of the public repeatedly provides information about a suspect to the Council, and that information is gained through a relationship with another person, this is potentially CHIS even if the Council has not asked them to do so.

3. Where should I go for advice?

If you need further advice after reading this guidance please contact Legal Services. See Appendix 1 for contact details.

4. What are the Different Types of RIPA Surveillance?

4.1. **Directed (Covert) Surveillance** – specifically focussing attention on an individual for the purposes of an investigation or operation conducted by the County Council. Directed surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware of it taking place and in circumstances where private information is likely to be gathered.

4.2. **Covert Human Intelligence Sources** – someone (a County Council officer or a member of the public) who provides information to the County Council by establishing or maintaining a relationship with a person to obtain information. The relationship is conducted in a manner to ensure that the person subject to the surveillance is unaware of it taking place.

5. Online covert activity – social media

5.1. It is just as important to consider the impact on an individual's privacy when investigating using social media, as when investigating 'on the ground'. Just because other people may also be able to see it, does not necessarily mean that a person has no expectation of privacy in relation to information posted on the internet. The fact that online investigation can be routine or easy to conduct does not reduce the need for authorisation.

5.2. The use of the internet may be required to gather information prior to and/or during an operation, and this may amount to directed surveillance if private information is likely to be obtained.

5.3. Viewing open source information (publicly available information), by attributable (see 5.8 below) means is unlikely to require authorisation under RIPA. An example is where privacy settings are available but not applied. However, the repetitive viewing of what are deemed to be open sources for the purposes of intelligence gathering or data collection may require an authorisation under RIPA and advice should be sought on individual cases.

5.4. The use of disguised purchaser details in a simple, overt, electronic purchase does not require a CHIS authorisation, because no relationship is usually established at that stage. However use of a false identity for a covert investigation may require a directed surveillance authorisation. Using photographs of a person without their permission to support a false identity infringes other law. Legal advice should always be sought.

5.5. Communicating covertly online may require a CHIS authorisation if a relationship is established. See Section 8 below regarding the use of CHIS and the Council's policy not to allow the use CHIS. The next paragraph explains when a CHIS scenario could arise.

5.6. The initial interaction involved in the act of bypassing privacy controls (for example the sending and acceptance of a friend's request) may be minimal. In many cases it is considered unlikely that this, by itself, will meet the RIPA

definition of a “relationship” and will not require authorisation as a CHIS. However, much work may have had to be

conducted to get to that stage without arousing suspicion. In addition, it may be difficult to predict how or at what pace that ‘relationship’ will need to develop. If it is intended or considered likely that direct one to one interaction with another person will go beyond the initial request/acceptance it would be appropriate to seek authorisation as a CHIS.

5.7. The creation of a false persona involving other ‘friends’, which are also false, in order to effect the deception and secure the information effectively amounts to ‘legend building’. Although this minimal initial interaction will not require authorisation as a CHIS it is considered good practice for ‘friends’ requests to be sent by a CHIS trained officer. Staff with access to covert social networking site profiles must not befriend other social networking site users in order to build the credibility of their profiles.

5.8. Any online research and investigation leaves a trace or ‘footprint’. A decision will therefore need to be made as to whether you wish to ensure that your research is non-attributable i.e. cannot be traced back to the Council or to identifiable individuals, or whether you are happy for it to be attributable i.e. capable of being traced back to the Council.

5.9. Due to traceability officers using the internet for investigative purposes must not use their own personal devices (PC, laptop, tablet, smart phone etc) as a means of accessing the internet.

5.10. Officers must not, under any circumstances, use their own personal social networking site profiles or other online accounts to undertake investigative research. There have been cases where such practices have resulted in the safety of officers and their families being seriously compromised.

5.11. The County Council has adopted a Social Media Policy and this should also be reviewed before considering an investigation using social media.

6. Key considerations when completing and authorising surveillance authorisations

6.1. **It is essential to record consideration of necessity in the authorisation form**. Where the information sought could be found by another means such as walking past and observing an address or asking a question, the use of surveillance will not be ‘necessary’. Or put another way, can the information be obtained openly? If the answer is yes, then the surveillance is not ‘necessary’ for the purpose of the investigation.

6.2. **It is essential to record consideration of proportionality in the authorisation form.** It is not enough to simply have a standard phrase saying that the surveillance is proportionate. The rationale for proceeding with covert surveillance needs to be written and explicit. The Office of the Surveillance Commissioner Guidance (2014) states at paragraph 73:

An authorisation should demonstrate how an Authorising Officer has reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (the proverbial 'sledgehammer to crack a nut'). Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, technique or tactic is the least intrusive. It is insufficient to make a simple assertion or to say that the 'seriousness' of the crime justifies any or every method available. It may be unacceptable to advance lack of resources or a potential cost saving as sufficient ground to use technological solutions which can be more intrusive than a human being. This critical judgment can only properly be reached once all other aspects of an authorisation have been fully considered.

6.3. Proportionality should include consideration of the following 3 elements: -

a) That the proposed covert surveillance is proportional to the mischief under investigation

b) That is it proportional to the degree of anticipated intrusion on the target and others, and

c) That it is the only option, other overt means having being considered and discounted

Authorising officers should consider the following **checklist** in framing responses to questions included in the application form: -

- What is the nature of the suspected or alleged offence/infringement?
- What, if any, are the alternatives to covert surveillance i.e. could the information be reasonably obtained by other means?
- If there are other options, why have these been rejected in favour of covert surveillance?
- What is the level of intrusion of privacy likely to be? Minimal? Average? Significant? Interference will not be justified if the means used to achieve the aim are excessive in the circumstances of the case. Further, any proposed interference with a person or persons' private home and family life should be carefully managed and must not be arbitrary or unfair
- Is the privacy of other persons not connected with the investigation likely to be effected? (collateral intrusion)
- What is the desired outcome?
- What is the anticipated benefit to the Council?

An authorisation should demonstrate how an Authorising Officer has reached the conclusion that the activity is proportionate to what it seeks to achieve; including an explanation of the reasons why the method, tactic or technique proposed is not disproportionate (the proverbial 'sledgehammer to crack a nut'). Proportionality is not only about balancing the effectiveness of covert methods over overt methods but of explaining why the particular covert method, technique or tactic is the least intrusive. It is insufficient to make a simple assertion or to say that the 'seriousness' of the crime justifies any or every method available. It may be unacceptable to advance lack of resources or a potential cost saving as sufficient ground to use technological solutions which can be more intrusive than a human being. This critical judgment can only properly be reached once all other aspects of an authorisation have been fully considered.

6.4. Proportionality in the context of RIPA authorisations has nothing to do with whether or not the possible benefits of a covert surveillance operation justify the time and money expended by the Council, although Officers no doubt wish to take this into account.

6.5. **In considering these principles it is important to take into account the risk of "collateral intrusion"**, i.e. intrusion on, or interference with, the privacy of persons other than the subject of the investigation. This is particularly important where there are special sensitivities, for example premises used by lawyers, doctors or priests for any form of medical or professional counselling or therapy. Steps must be taken to avoid unnecessary collateral intrusion and minimise any necessary intrusion into the lives of those not directly connected with the investigation or operation.

6.6. **Always use the form published on the Council's RIPA Intranet page which contains guidance** to help you make sure the right information is included. It is good practice for the officer requesting authorisation to discuss the application with the authorising officer.

7. Procedure for directed surveillance authorisations

7.1. **Before proceeding check the surveillance you are considering falls within the legal definition of directed surveillance.** Section 26(2) of RIPA defines surveillance as being directed if it is covert but not intrusive and is undertaken:

- for the purpose of a specific investigation or a specific operation,

- in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); **and**

- otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of RIPA to be sought for the carrying out of the surveillance.

7.2. Some of the terms above require further definition:

- **surveillance** is defined at Section 48(2-4) of RIPA as monitoring, observing or listening to persons, their movements, conversations, activities or communications

- **covert** has a dictionary definition including secret which in this context means unknown by the person under suspicion

- **intrusive** surveillance means involving the presence of an individual at residential premises or in someone's car, or using a surveillance device at residential premises or in someone's car. The County Council cannot authorise this type of surveillance under RIPA. The Office of the Surveillance

  Commissioner's guidance says that gardens and driveways are not included within the definition of "residential premises"

- **private information** in relation to a person includes any information relating to his/her private or family life as well as his/her professional or business affairs

7.3. The details of which officers can authorise directed surveillance in each Department are set out in Appendix 2.

7.4. The following steps must be followed by officers seeking authorisation for directed surveillance (all forms are available on the Council's RIPA Intranet page):

7.4.1. DS Application Form (Part II application for Authority for Directed Surveillance – the version with guidance notes available on the Intranet) will be completed by the Investigating Officer, checked by Legal Services and then submitted to an Authorising Officer.

7.4.2. If the Authorising Officer agrees to authorise the directed surveillance, after considering the requirements of Section 28 of RIPA and the guidance in the relevant RIPA Code of Practice, then he/she will authorise the surveillance activity in writing on the DS Application Form. If the approval is typed the Council needs to authenticate who the author was; for this reason hand-written authorisations are best practice.

7.4.3. Once the Authorising Officer has authorised the surveillance, the Investigating Officer who completed the application needs to contact the Magistrates Court to arrange a hearing for the authorisation to be approved. The Investigating Officer will be required to provide a copy of the original authorisation and the supporting documents setting out the case. A partially completed judicial application/order form will also need to be provided. At the hearing, which will be held in private, the Council cannot present any additional information as evidence, therefore the application must contain all the information that is relied on. The Authorising Officer, or if they are not

available the Investigating Officer, should attend the court hearing. In some circumstances it may be possible to arrange of an urgent out of hours hearing.

7.4.4. The Justice of the Peace will consider whether he/she is satisfied that at the time the authorisation was given there were reasonable grounds for believing that it was necessary and proportionate, and whether that continues to be the case. They will also consider whether the authorisation was given by the appropriate designate person at the correct level within the Council and whether the crime threshold has been met.

7.4.5. **Duration**: all written authorisations will continue until such time as they are formally CANCELLED. The duration of any directed surveillance authorisation is three months beginning on the date the Magistrate Court's approval is given.

7.4.6. **Review**: regular reviews must be undertaken using DS Review Form to avoid authorisations running on unnecessarily. Reviews should not broaden the scope of the investigation; in these circumstances a fresh authorisation may be required.

7.4.7. **Renewal:** if required DS Renewal Form will be submitted by the Investigating Officer to apply for an authorisation renewal at the expiry of the original authorisation. The Authorising Officer will consider the renewal application and if he/she is satisfied that the criteria are still met for the authorisation will renew the authority and endorse the DS Renewal Form. Any renewal must be approved by a Justice of the Peace in the same way the original authorisation was approved. Renewals should not broaden the scope of the investigation; in these circumstances a fresh authorisation may be required.

7.4.8. **Cancellation**: the officer who granted or last renewed the authorisation must cancel it if he/she is satisfied that the directed surveillance no longer meets the criteria for authorisation using the DS Cancellation Form. Authorisation should be for the minimum period reasonable for the purpose it is given and should be cancelled as soon as it is no longer required; this is a statutory requirement. As soon as the decision is taken to cancel, the instruction must be given to those involved to stop all surveillance. **It is important that every authorisation is cancelled, even if it has expired.**

7.4.9. All the above mentioned forms should be sent to the Coordinating Officer in Legal Services, within five working days of being signed-off.

7.4.10. It is the responsibility of the Coordinating Officer to maintain a central record of all authorisations for directed surveillance.

8. Covert Human Intelligence Sources (CHIS)

8.1. Legal advice must be sought straight away if CHIS circumstances have arisen, or where an investigation that might create a CHIS situation is being considered. The following information is provided to ensure officers can recognise a CHIS situation.

8.2. Section 26(8) of RIPA defines a person as being a covert human intelligence source (CHIS) if he/she establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within the following two paragraphs:

- he/she covertly uses such a relationship to obtain information or to provide access to any information to another person; or

- he/she covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship

8.3. A member of the public volunteering information to the Council would not at that stage be a covert human intelligence source but it would become a CHIS situation if he/she was encouraged to gather further information through a relationship that fits the Section 26(8) definition. Even if an individual is not encouraged to gather information this way and is not specifically tasked to do so, if the Council will potentially use the information there could be a duty of care to that individual, and the onus is on the Council to manage the source properly. When an informant gives repeat information about a suspect and it becomes apparent that the informant may be obtaining the information in the course of a neighbourhood or family relationship for example, it may mean that the informant is in fact a CHIS.

8.4. Communicating covertly online may require a CHIS authorisation if a relationship is established. Please refer back to 'Online covert activity – social media' at paragraph 5 for further guidance.

8.5. Special caution should be exercised in relation to the following groups and the Council's Chief Executive is the only person with authority to authorise CHIS applications relating to these groups :

8.5.1. the use of juveniles (people under the age of 18) as covert human intelligence sources requires consideration to be given to the requirements of the Regulation of Investigatory Powers (Juveniles) Order 2000 and the relevant RIPA Code of Practice. On no occasion should the use or conduct of a source under the age of 16 be authorised to give information against their parents or any person who has parental responsibility for them.

8.5.2. vulnerable individuals, such as the mentally impaired or someone who is vulnerable by virtue of their age or disability, should only be authorised to act as a source in the most exceptional circumstances;

9. Important Further Information relating to CHIS

9.1. The Council would be responsible for safeguarding the wellbeing of anyone authorised as a CHIS. The requirements are onerous. If a situation arose where a CHIS was made known to the Council that person should be redirected to the Police if possible. The following information is provided to ensure officers understand the serious implications of CHIS scenarios and to ensure they are equipped to act as a 'handler' or 'controller' if a CHIS situation arises that cannot be redirected to the Police.

9.1.1. Management of Sources: every source should have a designated handler which will normally be the Investigating Officer applying for the authorisation.

9.1.2. "Handler" means the person referred to in Section 29(5)(a) of RIPA who will have day to day responsibility for:

- dealing with the source on our behalf;

- directing the day to day activities of the source;
- recording the information supplied by the source;
- monitoring the source's security and welfare.

9.1.3. Also every source should have a designated controller which would normally be the line manager of the Investigating Officer.

9.1.4. "Controller" means the officer referred to in Section 29(5)(b) of RIPA, responsible for the general oversight of the use of the source.

9.1.5. Tasking: tasking is the assignment given to the source by the handler or controller, asking him/her to obtain information, or to otherwise take an action leading to the obtaining of information.

9.1.6. When unforeseen actions or undertakings occur when a handler meets a source, or the source meets the target of an investigation, any such actions or undertakings must be recorded as soon as practicable after the event and, if the existing authorisation is insufficient, a new authorisation should be obtained before any further such action is carried out.

9.2. Security and Welfare: before authorising the use or conduct of a source, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the source become known to the target of the investigation or others. The ongoing security and welfare of the source, after the end or cancellation of the authorisation, should also be considered at the outset.

9.3. The handler is responsible for bringing to the controller's attention any concerns about the personal circumstances of the source, insofar as they might affect:

- the validity of the risk assessment;
- the proper conduct of the source operation;

- the safety and welfare of the source.

9.3.1. Any such concerns must be brought to the attention of the Authorising Officer by the controller and a decision taken on whether or not to allow the authorisation to continue. Please note that the Authorising Officer might be the controller.

9.4. Record keeping: Records must be maintained in such a way as to preserve the confidentiality of the source and the information provided by that source. The records should contain the particulars as set out in the relevant RIPA Code of Practice, and these should be made and updated by the Investigating Officer and the relevant records or updates must be sent to the Coordinating Officer within five working days. Records that disclose the identity of a source will not be made available to other officers except where a need for access is demonstrated.

10. Procedure for CHIS Authorisations – not to be undertaken before legal advice is taken

10.1. In the unlikely event of a CHIS authorisation being required the procedural guidance in this section should be followed after first seeking legal advice.

10.2. The details of which officers can authorise the use of CHIS are set out in Appendix 2.

10.3. The following steps must be followed by officers seeking authorisation for the use or conduct of a CHIS (all forms are available on the Council's RIPA Intranet page):

10.3.1. CHIS Application Form (Part II application for authorisation of the use or conduct of a CHIS) will be completed by the Investigating Officer, checked by Legal Services and then submitted to an Authorising Officer.

10.3.2. If the Authorising Officer agrees to authorise the use or conduct of a covert human intelligence source, after considering the requirements of Section 29 and the guidance in the relevant RIPA Code of Practice, then he will authorise the use of the covert human intelligence source in writing on the CHIS Application Form If the approval is typed the Council needs to authenticate who the author was; for this reason hand-written authorisations are best practice.

10.3.3. The Authorising Officer must also complete a Source Identity form, ensuring that the Operation Reference Number corresponds with that on the CHIS Application Form.

10.3.4. Once the Authorising Officer has authorised the CHIS, the Investigating Officer who completed the application needs to contact the Magistrates Court to arrange a hearing for the authorisation to be approved. The Investigating Officer will be required to provide a copy of the original authorisation and the supporting documents setting out the

case. A partially completed judicial application/order form will also need to be provided. At the hearing, which will be held in private, the Council cannot present any additional information as evidence, therefore the application must contain all the information that is relied on. The Authorising Officer, or if they are not available the Investigating Officer should attend the court hearing. In some circumstances it may be possible to arrange of an urgent out of hours hearing.

10.3.5. The Justice of the Peace will consider whether he/she is satisfied that at the time the authorisation was given there were reasonable grounds for believing that it was necessary and proportionate, and whether that continues to be the case. They will also consider whether the authorisation was given by the appropriate designate person at the correct level within the Council

10.4. In relation to a covert internet investigations, it may not be possible to construct a single authorisation to cover all of the relationships because the

persons with whom relationships are established are not known in advance. In such a situation it will be necessary to construct separate authorisations. It is important that the same Authorising Officer considers each authorisation to ensure that operational conflict and risks do not develop, and to monitor the security and welfare of the CHIS. Where appropriate, reviews should be combined to reduce bureaucracy and error.

10.5. **Duration:** all written authorisations will continue until such time as they are formally cancelled. A CHIS authorisation is for a period of **12 months** beginning on the date the Magistrate Court's approval is given or **4 months** for juvenile sources and vulnerable individual sources.

10.6. **Review:** Regular reviews must be undertaken using CHIS Review Form to avoid authorisations running on unnecessarily. Juvenile sources and vulnerable individual sources will be reviewed no later than 28 days after the granting of an authorisation. Reviews should not broaden the scope of the investigation; in these circumstances a fresh authorisation may be required.

10.7. **Renewal:** If required, the CHIS Renewal Form will be submitted by the Investigating Officer to apply for an authorisation renewal at the expiry of the original authorisation. Before an Authorising Officer renews an authorisation, he/she must be satisfied that a review has been carried out of the use made of the source during the period authorised, the tasks given to the source and the information obtained from the use or conduct of the source. The key issue to consider is the risk involved in the operation to the source. If the Authorising Officer is satisfied that the criteria for the initial authorisation continue to be met, he/she may renew the authorisation and endorse the CHIS Renewal Form. Any renewal must be approved by a Justice of the Peace in the same way the original authorisation was approved. Renewals should not broaden the scope of the investigation; in these circumstances a fresh authorisation may be required.

10.8. **Cancellation:** the officer who granted or last renewed the authorisation must cancel it using the CHIS Cancellation Form if he/she is satisfied that the use or conduct of the source no longer satisfies the criteria or that the arrangements for oversight and management of the source are no longer in place. Authorisation should be for the minimum period required for the purpose it is granted and should be cancelled as soon as no longer required; this is a statutory requirement. As soon as the decision is taken to cancel, the instruction must be given to those involved to stop all activity authorised by the CHIS. **It is important that every authorisation is cancelled, even if it has expired.**

10.9. All the above mentioned forms should be sent to the Co-Ordinating Officer in Legal Services, within five working days of being signed-off.

10.10. It will be the responsibility of the Co-Ordinating Officer to maintain a central record of all authorisations for CHIS.

12. Record Keeping and Central Record of Authorisations

12.1. In all cases in which authorisation of directed surveillance and the use of a covert human intelligence source is sought, the individual department is responsible for ensuring that the documentation is sent to the Coordinating Officer who will keep it for a period of at least three years from the date of authorisation and always for at least one Office of the Surveillance Commissioner (OSC) inspection. These records will be available for inspection by the OSC.

12.2. The Coordinating Officer will arrange for and regularly update a centrally retrievable record of all applications in accordance with the Code of Practice. In all cases the documentation specified by the Code of Practice will be retained.

12.3. The investigating department must ensure that appropriate arrangements are in place for the handling, storage access and destruction of material obtained through the use of covert surveillance.

12.4. The Coordinating Officer is responsible for submitting required reports to the OSC, including any activity that is not properly authorised.

13. Confidential Material

13.1. Particular attention is drawn to areas where the subject of surveillance may reasonably expect a high degree of privacy, or where confidential information may be involved. Examples of “Confidential Material” include:

13.1.1. confidential personal information – this will include physical and mental health information held by healthcare professionals and spiritual counselling information held by Ministers of religion;

13.1.2. confidential journalistic material – this is information obtained for journalistic purposes subject to an undertaking that it will be held in confidence;

13.1.3. communications subject to legal privilege;

13.1.4. communications between an MP and another person on a constituency matter.

13.2. Where any authorisation is likely to result in the acquisition of or knowledge of confidential material, the authorisation can only be considered by the Council's Chief Executive, or in their absence a Chief Officer (Corporate Director). Legal advice should be sought where information is considered to be confidential.

13.3. The general principles applying to confidential material acquired under RIPA Part II authorisation are:

13.3.1. those handling material from such operations should be alert to anything which may fall within the definition of confidential material. Where

there is doubt as to whether the material is confidential, advice should be sought from the appropriate Authorising Officer and Legal Services before further dissemination takes place;

13.3.2. confidential material should not be retained or copied unless it is necessary for a specified purpose;

13.3.3. confidential material should be disseminated only where an appropriate Authorising Officer is satisfied that it is necessary for a specific purpose;

13.3.4. the retention or dissemination of such information should be accompanied by a clear warning of its confidential nature. It should be safeguarded by taking reasonable steps to ensure that there is no possibility of it becoming available, or its content being known, to any person whose possession of it might prejudice any criminal or civil proceedings related to the information;

13.3.5. confidential material should be destroyed (or securely deleted if the record is electronic) as soon as it is no longer necessary to retain it for a specified purpose;

13.3.6. where confidential material has been acquired and retained, the matter should be reported to the Commissioner or Inspector during his next inspection.

APPENDIX 1 – useful contacts